On the Integration of Security and Dependability in Computer Systems*

Erland Jonsson, Tomas Olovsson
Department of Computer Engineering
Chalmers University of Technology
S-412 96 Gothenburg, SWEDEN
email: jonsson@ce.chalmers.se

ABSTRACT

Historically the trustworthiness of a computer system was characterized by its reliability and availability. Later on safety was integrated into what is now termed dependability. System security was originally a concept that described the protection of information from intentional and hostile interaction. It has now been suggested that security should be treated as a dependability attribute, parallel to reliability, availability and safety, but the implications of this integration has not yet been fully realized. This paper presents a novel approach to security, intended to facilitate and improve this integration. This is accomplished by taking a dependability viewpoint on traditional security and interpreting it in terms of system behaviour and fault prevention. A modified security concept, comprising only fault prevention characteristics and a new behaviouristic concept, privacy, are defined. The outcome of this interpretation will influence the integration of the other three dependability attributes.

Keywords: Computer System, Dependability, Security, Concepts, Terminology.

1. INTRODUCTION

The research field of security and dependability are two disciplines that describe important properties of computer systems. In short, security has emerged from the viewpoint of intentional and hostile interaction with a database system, so that unauthorized disclosure or modification of information results. Dependability has evolved from reliability and availability considerations. Security and dependability have traditionally been treated separately. Lately however, attempts have been made to integrate these two, e.g as suggested in [14], where dependability is defined as the overall concept of which security is just an attribute among others. However, the consequences of this proposed integration have not yet been fully realized. What we are facing here is the classical problem of two successful disciplines that are both evolving, resulting in a situation where an overlap occurs.

* This work was supported by the PDCS (Predictably Dependable Computing Systems) of the European ESPRIT program, under contract #90-02692P from the Swedish National Board for Industrial and Technical Development (NUTEK).

Advocates for each discipline tend to incorporate the “other” into their “own” one without realizing the changes that such an integration would entail. The incorporation of security as a dependability attribute has already been mentioned. Similar attempts can be found within the security community [6].

Another point of concern is that the concepts overlap and that each discipline uses a set of viewpoints and a terminology that is often incompatible with that of the other discipline.The most striking example of overlap is availability. From the security viewpoint it describes the possible disruption of service delivery to the authorized user as a result of intentional interaction. However, from the reliability viewpoint the possible service disruption is normally due to a component failure, even if no restriction with respect to the cause is really made.

An illustration of a discrepancy in terminology is that in the dependability discipline reasons for *failures* are called *faults*, whereas security people talk about *attacks* that cause *breaches*. Whether these terms correspond directly is not clear, even if the similarity is evident. A lot of questions of this type could be posed. What are the relations between e.g. fault, attack, flaw, error, bug, vulnerability, defect? Do some of these terms represent identical concepts? Should we in that case look for unification of terminology, or is it justifiable to maintain separate terminologies for each discipline? These are questions which need to be answered as integration work proceeds, and even though a full answer will not be given in this paper the suggestions made will considerably facilitate further work in this direction.

2. PRESENT STATUS

This section gives the present status of the disciplines of dependability and security. There are many different opinions as to the status of discussion of the concepts and terminology used. The versions given below are believed to have a widespread acceptance. Dependability is given in its ”classical” form with the traditional way of integrating security. Security is described by its different aspects and some alternatives are mentioned. It should be noted that there are two main security concepts. The first one is related to database systems and information security. The second one can be related to any com-

puter system or even any system at all and includes all types of security. The first concept can be seen as a subset of the second.

2.1 Security and its aspects

The security of a computer system is normally understood as its ability to withstand illegal intentional interaction or attacks against *system assets* such as data, hardware or software. This notion of security normally assumes a hostile action from a person, the *attacker*, who often tries to gain some kind of personal benefit from his actions. Security is normally defined by three different aspects: *confidentiality, integrity* and *availability* [8], [9], [14], [17].

Confidentiality, which is also called *secrecy*, is the ability of the computing system to prevent unauthorized access to system assets, such as the disclosure of information to unauthorized parties. *Integrity* is the ability of the computer system to prevent data or other assets from being modified, deleted or destroyed by an unauthorized party. Finally, *availability*, is the system's ability to deliver its normal service to the authorized user, even in the presence of attacks.

Various versions of the definition of security exist. Some authors add one or two extra aspects, such as *denial-of-service* and *authenticity*, others prefer a different grouping, see e.g. [11], [15]. In database systems *integrity* refers to actions taken by an authorized party and to the accuracy and validity of data, whereas *security* refers to protection of data against unauthorized interaction [5].

Finally, there exists a completely different security concept, which is mainly applicable for information or data security. This concept concentrates on the development procedure and defines security in formalistic terms as a method for enforcement of a *security policy* for a company or organization. The security policy is understood as a set of laws, rules and practices that regulates how an organization manages, protects and distributes sensitive information [7], [9].

2.2 Dependability and its attributes

Dependability was first introduced as an extension of *reliability* and *availability* and these were then reduced to be specific attributes of dependability together with *safety* and *security* [13]. Reliability and availability constitute different views of a basic concept that deals with the delivery of *service*. Here, service is the system behaviour as perceived by its users [14]. Reliability is a characteristic that reflects the probability that the system will deliver its service under specified conditions for a stated period of time, whereas availability reflects the probability that the system will be available, or ready for use, at a certain instant in time. Availability describes the system in terms of the alternation between operating periods and periods of failure. Thus availability, as opposed to reliability, incorporates the fact that a system can be repaired.

At a later date the attribute of *safety* was added. Safety is also related to the service delivered by the system, but rather than characterizing the system during operation, it denotes the system's ability to fail in such a way that catastrophic consequences are avoided. Safety is reliability with respect to catastrophic failures.

Finally it was suggested that *security* be incorporated as a fourth dependability attribute. It refers to the system's ability to prevent unauthorized access and/or handling of information [14]. However, as we shall see in the following, security is a more complex concept than reliability and availability are, and some aspects of security clearly overlap already existing reliability/availability aspects. Therefore, security integration into dependability calls for some adaptation of both concepts.

3. A SYSTEM MODEL FOR DEPENDABILITY

3.1 Background

In this section we shall define a simple system model aimed at illustrating some basic properties of dependable computer systems and which we shall then use to describe how security can be better integrated into dependability.

In general, there are two basic types of interaction between a system and its environment, see figure 1. First, the system affects the environment or is delivering an output to the environment, which experiences the output as the *system behaviour*.

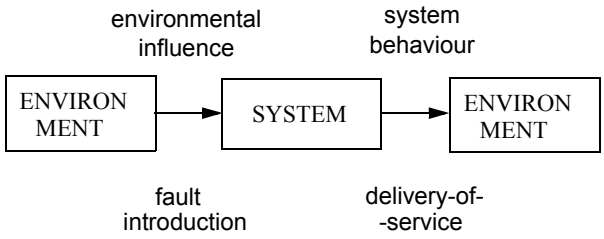

Figure 1: A system model for dependability

There is also an *environmental influence* on the system, which means that the system receives an input from the environment. The input consists of many different types of interaction. The type of interaction we are interested in here is interaction that involves a *fault introduction* into the system. Since faults are detrimental to the system, we seek to design the system so that the introduction of faults is prevented*: fault prevention.*

3.2 System behaviour and dependability

A closer look closer at the system behaviour will show that we need to distinguish between three different receivers of the output delivered by the system: the authorized user, the unauthorized user, and the rest of the environment of the system. See figure 2. The authorized users are the users that are the intended receivers of the service that the system delivers, as specified in the system specification. In the following we shall call the authorized user(s) the **User**. A user is any system in the environment that is a potential consumer of the output delivered by the system. It may be human or object: a person, a computer, a program etc. All potential users except the autho-

rized users are unauthorized users. Unauthorized users are called **Non-users.** The third receiver is the rest of the environment of the system, which we call **Other environment**. Thus, the environment consists of the Users, the Non-users and the Other environment.

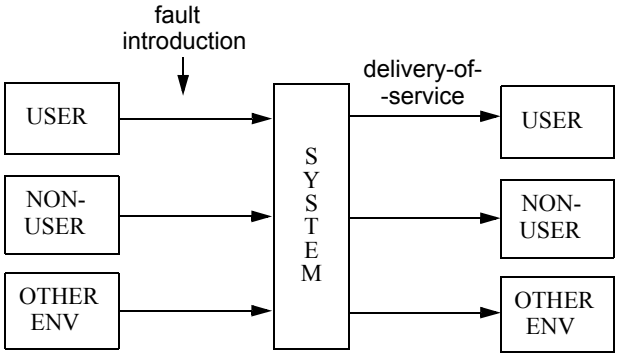

Figure 2: System dependability interaction with environment

We observe that dependability is defined as "the trustworthiness of a computer system such that reliance can justifiably be placed on the service it delivers", where the service is the system behaviour as perceived by the user(s) [14]. In this definition it is understood, even if not explicitly stated, that the user(s) are the authorized user(s). Thus dependability is defined in terms of service delivery to the User. Nothing is said about delivery of service to Non-users or to the Other environment, nor about other types of output to the environment other than the specified service.

3.3 Fault introduction

The receivers of the system output normally also create an input to the system. Thus they are potential sources for fault introduction: faults may originate from the User, the Non-user or the Other environment. See figure 2.

Here, the term *fault* is used in the sense of an event-type phenomenon that leads to an error in the system and that may eventually result in unwanted system behaviour, i.e. a failure or security exposure. The faults considered here are external faults, the sources of which are found in the environment. External "classical" faults of all types, as well as security attacks, are included in this definition. A fault made by a User may be an accidental handling fault. An example of a Non-user fault is an intentional security violation. Ionizing radiation from other subsystems in the environment may also cause faults.

4. UNDERSTANDING SECURITY IN DEPENDABILITY TERMS.

4.1 Background

Given the system model for dependable systems in the previous section, we now ask ourselves how the traditional security concept could be readily interpreted in dependability terms. We shall see in the following that the three aspects, confidentiality, integrity and availability are, to a large extent, already covered by existing concepts in the dependability discipline, either as a *behaviouristic* concept, i.e. related to the behaviour of the system, or as a *preventive* concept, i.e. related to the prevention of faults from being introduced into the system.

4.2 Availability

Availability is primarily defined as the ability of the system to deliver its service to the User, i.e. a behaviouristic concept. Therefore, availability as a security aspect is clearly a subset of the availability concept in dependability. See figure 3.

Availability also includes the prevention of faults from being introduced by a Non-user, which would lead to a situation in which the service is no longer available to the user. This is a fault prevention issue with respect to intentional interaction faults made by the Non-user. Consequently, availability as a security aspect is completely covered by the corresponding dependability attribute.

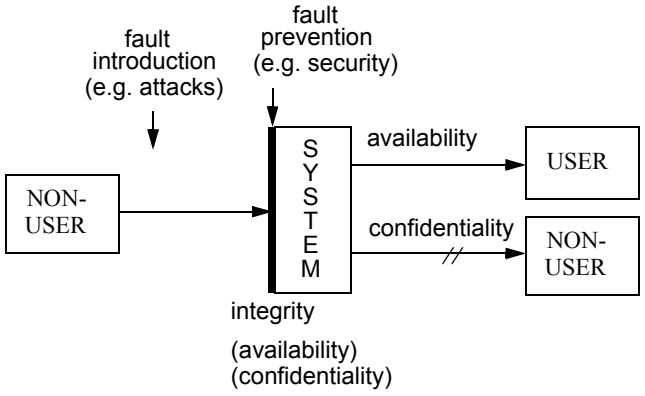

Figure 3: Understanding security in dependability terms

4.3 Integrity

Integrity is the prevention of unauthorized modification, deletion or destruction of system assets. Integrity is violated by means of an attack, which is normally performed by a Non-

user, but may also be performed by a User who is abusing his authority. (Note that in database literature integrity is exclusively related to User action.)

Thus, integrity is a preventive quality of a system and characterizes the system's ability to withstand attacks. If the prevention is not successful, reduced availability would normally result. This preventive quality is built into the system, either technically and/or as a part of the regulatory mechanisms that protects the system. Thus, integrity describes some of the means for fault prevention that are available to a system. Therefore, integrity is also covered by well-known dependability concepts.

4.4 Confidentiality

Confidentiality is the ability of the system to prevent unauthorized access to system assets, i. e. restricting the availability of the service delivered by the system to the Non-users.

It is thus a behaviouristic concept which defines certain characteristics of the system behaviour, but unlike other attributes it defines *system behaviour with respect to a Non-user*. It actually defines to what extent information and other assets should be accessible, or rather not accessible, to Non-users. Therefore, the behaviouristic aspect of confidentiality can be regarded as a new attribute in the dependability discipline, parallel to reliability, availability and safety.

Sometimes, confidentiality also has a preventive meaning, i.e. how to prevent Non-user fault introduction that would e.g. lead to an unauthorized disclosure of information.

4.5 Security

In view of the discussion in the previous sections we suggest a modified definition of the security concept, so that security is simply regarded as a form of fault prevention, namely fault prevention with respect to intentional faults. Thus, security is a purely preventive concept, which is not at all related to the behaviour of the system but only to its ability to protect itself against certain types of faults and attacks. Consequently, *security mechanisms* are fault prevention mechanisms and a *security policy* informs about the security mechanisms that are needed in order to ensure an unimpaired system behaviour.

5. MODIFIED DEPENDABILITY ATTRIBUTES

The preceding section suggested that the behaviouristic part of confidentiality should be defined as a separate dependability attribute that would describe the relation of the computer system to the Non-user. One could discuss what word to use for this new attribute. In order to avoid confusion caused by terms already used in the traditional security context, such as e.g. "confidentiality" or even "security", we have chosen to use the word **privacy**. The advantage of this word is that it includes meanings such as confidentiality and secrecy, which are appropriate for information privacy, but also the meaning seclusion, which could stand for privacy of assets such as hardware and software. See figure 4.

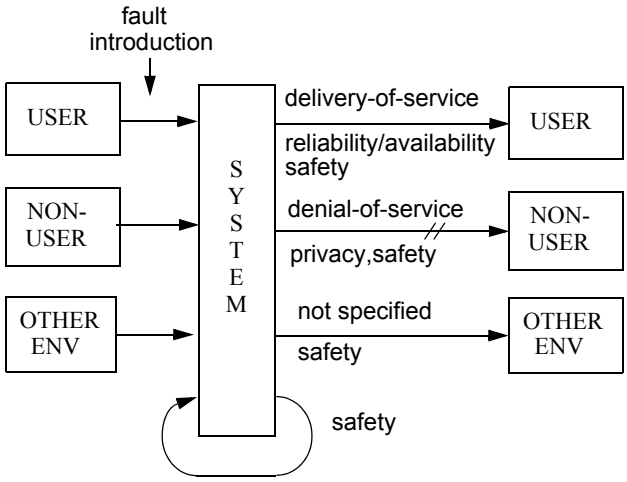

Figure 4: Modified dependability attributes

Reliability and availability, on the other hand, are both attributes describing the relation of the computer system to the User. They could therefore be regarded as views on the same composite attribute: reliability/availability.

Where does that leave safety? With the proposed terminology safety could be expressed as the system's ability to fail in such a way that unintended catastrophic consequences are avoided, whether those consequences would affect the User, Non-user, Other environment or the system itself. If we take the viewpoint of the User and Non-user, safety could be regarded as a "sub-attribute" to either reliability/availability or privacy. This would mean that dependability would be understood in terms of only two attributes: reliability/availability (related to the User) and privacy (related to the Non-user), leaving safety to describe certain types of failures for both of these. However, due to the importance of safety properties and in order to clearly incorporate their possible impact on the system itself and on the Other environment, we have chosen to present safety as a separate attribute. See figure 5.

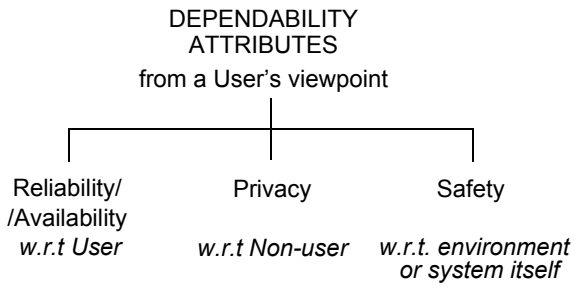

Figure 5: Dependability attributes from a User's viewpoint

The modified definitions of dependability and its attributes can be summarized as follows:

reliability/availability: refers to the system's ability of delivery-of-service to the authorized users, called Users.

privacy: refers to the system's ability of denial-of-service to unauthorized users, called Non-users. All users but those explicitly specified as authorized users are Non-users.

safety: refers to the system's ability to avoid unintended catastrophic consequences. These consequences may affect the environment, including Users, Non-users and the Other environment, or the system itself.

dependability: is the trustworthiness of a computer system such that reliance can be justifiably placed on the service it delivers to its Users, on the privacy it maintains with respect to its Non-users and on the absence of unintended catastrophic consequences.

Unfortunately, in the definition of safety, the word "unintended" has to be added since many systems are constructed to intentionally cause catastrophic consequences on the environment, an obvious example being warheads.

6. CONCLUSIONS

A novel approach to the integration of security and dependability has been proposed. It is based on the observation that the dependability of a computer system could be described in behaviouristic and preventive terms. A behaviouristic viewpoint is related to the behaviour of the system, i.e. to how the system influences its environment. A preventive viewpoint describes the measures to be taken to prevent faults from being introduced into the system, i.e. how to prevent unwanted environmental influence on the system.

Using this approach we have shown how the various aspects of traditional security could either be mapped onto existing dependability concepts or be understood as a new dependability attribute, which we call privacy. The meaning of privacy is quite close to that of confidentiality, but includes only the behaviouristic part of it. Privacy is different from the existing dependability attributes in that it describes the system's relation to an unauthorized user, whereas the composite reliability/availability attribute describes the relation with the authorized user. Safety describes the system's ability to avoid catastrophic failures whether reliability or privacy failures.

Security is redefined as a concept for fault prevention with respect to intentional external faults or attacks against the system with no specific relation to behaviouristic attributes, such as privacy or reliability/availability.

7. REFERENCES

[1] **T. Anderson** (editor)**:** *Safe & Secure Computing Systems*, Blackwell Scientific Publications, ISBN 0-632-01819-4, 1989.

[2] **R. H. Baker:** *Computer Security Handbook, 2nd Edition*, TAB Professional and Reference Books, McGraw-Hill Inc, ISBN 0-8306-7592-2, 1991.

[3] **T. Beth, J. Dobson, D. Gollman, A Klar:** "Security Evaluation Report: Concepts and Terminology*,"* EISS-Universität Karslruhe / University of Newcastle upon Tyne, 1990.

[4] **L. Blain, Y. Deswarte:** "An Intrusion-tolerant Security Server for an open Distributed System," LAAS report no 90085, March 1990, Toulouse, France.

[5] **C. J. Date:** *An Introduction to Database Systems, vol. 1, 5th edition,* pp. 429ff. Addison-Wesley 1990, ISBN 0-201-51381-1.

[6] **D.E. Denning:** "Secure Databases and Safety: Some unexpected conflicts," pp. 101-111 in T. Anderson (editor): *Safe & Secure Computing Systems,* Blackwell Scientific Publications, ISBN 0-632-01819-4, 1989.

[7] **Department of Defence:** *Trusted Computer System Evaluation Criteria* ("orange book"), CSC-STD-001-83.

[8] **D. K. Hsiao:** "Database Security Course Module," pp. 269-301 in *Database Security: Status and Prospects,* Elsevier Science Publishers B.V, Holland, IFIP WG 11.3, ISBN 0-444- 70479-5, 1988

[9] **Information Technology Security Evaluation Criteria (ITSEC)**: *Harmonized Criteria of France-Germany-the Netherlands-the United Kingdom,* Draft 1990. Kollen-Druck Bonn.

[10] **International Standards Organization:** *Data Processing - Open Systems Interconnection - Basic Reference Model,* ISO/IS 7498, Geneva 1983.

[11] **International Standards Organization:** *Information processing systems - Open Systems Interconnection - Basic Reference Model, part 2: Security Architecture 7498/2*.

[12] **M.K. Joseph:** "Integration problems in Fault-tolerant, secure computer design*,"* pp. 347-364 in A.Avizienis. J.C. Laprie (editors): *Dependable Computing for Critical Applications,* Springer-Verlag, N.Y., ISBN 3-211-82249-6, 1991.

[13] **J.C. Laprie**: "Dependable Computing and Fault Tolerance: Concepts and Terminology," in *Proc. 15th IEEE International Symposium on Fault-Tolerant Computing (FTCS-15), June 1985.*

[14] **J.C. Laprie et al.:** *Dependability: Basic Concepts and Terminology,* Springer-Verlag, ISBN 3-211-82296-8, 1991.

[15] **S. Muftic:** *Security Mechanisms for Computer Networks,* Ellis Horwood Ltd, England, ISBN 0-7458-0613-9, 1989.

[16] **D. M. Nessett:** "Factors Affecting Distributed System Security," *IEEE Symp. on Security & Privacy,* 1986, pp. 204 - 222.

[17] **C. P. Pfleeger:** *Security In Computing,* Prentice Hall International, Inc. ISBN 0-13-799016-2, 1989.